Application No. 09/973,769 Attorney Docket No. T3497-9052US01



**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application.

**Listing of Claims:**

Claims 1-28 (Cancelled).

29. (previously presented) A security device for installation at a node of a digital network, said security device comprising:

a security engine for providing user transparent communications to another node of said digital network;

at least two locking devices, wherein each locking device is coupled to the other locking devices and the security engine, and each locking device is configured to communicate with the other locking devices and with the security engine; and

a programmed data processor including a memory to store data corresponding to said user communications and to store an embedded security policy manager and a manager object and at least one managed object, wherein the managed object is configured to detect communications at a first node having a characteristic which differs from a normal usage characteristic and to send an alarm through the manager object to said security engine for communication to a managed object of a second node, the managed object corresponding to said first node, as said user transparent communications

and for responding to user transparent communications from said second node of said digital network and controlling of routing of communications in said digital network wherein said first node and said second node are hierarchically arranged locally in said digital network and arranged to provide redundant connections between nodes at different hierarchical levels.

Claims 30-34 (Cancelled).

35. (previously presented) A digital network for active intrusion resistance, said digital network comprising:

a plurality of nodes arranged in a tiered hierarchy, each node including

at least two locking devices;

a security policy manager device for detecting network communications or activity having a characteristic different from a normal usage characteristic and providing a signal to other network nodes; and

a communication module responsive to a user transparent signal from another node for controlling said at least two locking devices to isolate a node by selecting from among redundant communication paths in said digital network to maintain network communications between nodes that are not to be isolated and restricting communications with a node to be isolated, whereby the digital network actively resists intrusion by isolating one or more nodes that are determined to have become untrusted.

36. (previously presented) A digital network as recited in claim 35, wherein each node

further includes a memory to store data corresponding to said user transparent communications and to store an embedded security policy manager, a manager object, and managed objects corresponding to each connected node.

37. (previously presented) A digital network as recited in claim 35, wherein said controlling of said at least two locking devices to isolate a node of said digital network is performed in real time.

38. (previously presented) A digital network as recited in claim 35, wherein said tiered hierarchy includes redundant connections between nodes at different levels in the hierarchy.

39. (previously presented) A digital network as recited in claim 35, wherein each node further includes a module for defining a secure session between nodes.

40. (previously presented) A digital network as recited in claim 39, wherein said module for defining a secure session includes a portion to transmit information corresponding to one of an authenticated user and an identification of a communicating node, wherein the identification of the communicating node can be used to isolate nodes corresponding to the secure session such that the digital network actively resists intrusion by compartmentalizing untrusted nodes within the secure session.

41. (previously presented) A digital network as recited in claim 35, wherein said

characteristic which differs from said normal usage characteristics is a potential attack characteristic.

42. (previously presented) A digital network as recited in claim 35, wherein said characteristic that differs from said normal usage characteristic corresponds to a fault at a node or link of said digital network.

43. (previously presented) A digital network as recited in claim 35, wherein said manager object manages said managed object, and wherein each managed object corresponds to any external node coupled to each node.

44. (previously presented) A method of actively resisting intrusion in a digital network using extensions to an object request broker, said method comprising:

providing object request broker software;

extending the object request broker software to include encryption, intrusion detection, and security policy management and enforcement;

generating a manager object on one or more nodes and at least one managed object on each node;

detecting, with a managed object, a communication having a characteristic differing from a normal usage characteristic at a first node of said digital network, said communication received from a second node of said digital network;

communicating a user transparent signal from a managed object of the first node to a managed object of a third digital network node responsive to said detection; and

controlling communications, through coordinated managed and manager objects, at said first node and said third node to restrict communications from said second node with a user transparent signal.

45. (previously presented) A method as recited in claim 44, wherein said step of controlling communications includes steps of

isolating said second node from said digital network to restrict untrusted communications from the second node from being allowed onto the digital network, and

routing other digital network communications through redundant links between nodes of said digital network so as to bypass and isolate the second node.

46. (previously presented) A method as recited in claim 44, wherein said detecting step is performed by the managed object at the first node of said digital network and said controlling step is performed responsive to the managed object at said third node of said digital network.

47. (previously presented) A method as recited in claim 44, wherein said detecting, communicating and controlling steps are performed in substantially real time.

48. (previously presented) A method as recited in claim 44, including a further step of defining a secure session between a plurality of nodes in a communication path in said digital network, wherein said secure session allows compartmentalization of any untrusted nodes.